

LLM's revisions of  drafts --  
14 Nov 72

25X1

DRAFT:JDM:bg  
10 November 1972

NATIONAL SECURITY ACT AMENDMENTS OF 1973

CHAPTER \_\_\_\_\_ --PUBLIC LAW \_\_\_\_\_

/H.R. \_\_\_\_\_/

An Act to protect the security of the foreign intelligence  
activities of the United States

Be it enacted by the Senate and House of Representatives of the United  
States of America in Congress assembled,

Section 1. This Act may be cited as the National Security  
Act Amendments of 1973.

Section 2. Section 102 of the National Security Act of 1947,  
as amended, is amended by adding a new subsection (g) to read as  
follows:

(g) In the interests of the security of the foreign  
intelligence activities of the United States and in order  
further to implement the proviso of section 102(d)(3) of  
this Act that the Director of Central Intelligence shall be  
responsible for protecting intelligence sources and methods

from unauthorized disclosure--

(1) The Director of Central Intelligence shall have authority to issue rules and regulations for the protection of intelligence sources or methods from unauthorized disclosure and shall provide for the classification as "Sensitive Intelligence Sources and Methods" of any information of any kind:

a. revealing the existence or nature of either a source or method for collecting foreign intelligence information or materials, and

b. the unauthorized disclosure of which could lead to counteraction jeopardizing the productivity of such sources or methods.

(2) Whoever, being or having been an officer or employee of the United States Government, or being or having been a contractor of the United States Government, or being or having been an employee of a contractor of the United States Government, and in the course of such relationship becomes entrusted with "Sensitive Intelligence Sources and Methods" information, knowingly communicates or causes to be communicated such information or any part thereof to an unauthorized person shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(3) The term "unauthorized person" means any person or agency not authorized by the President or by the Director of Central Intelligence with the approval of the President to receive such information classified "Sensitive Intelligence Sources and Methods."

(4) Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts or practices which constitute, or will constitute, a violation of this section, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with the provisions of this section or any regulation or order issued thereunder, and upon a showing by the Director of Central Intelligence that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted.

DRAFT:JDM:bg  
10 November 1972

NATIONAL SECURITY ACT AMENDMENTS OF 1973

CHAPTER \_\_\_\_\_ --PUBLIC LAW \_\_\_\_\_

[H. R.        ]

An Act to protect the security of the foreign intelligence  
activities of the United States

Be it enacted by the Senate and House of Representatives of the United  
States of America in Congress assembled,

Section 1. This Act may be cited as the National Security Act  
Amendments of 1973.

Section 2. Section 102 of the National Security Act of 1947,  
as amended, is amended by adding a new subsection (g) to read as  
follows:

(g) In the interests of the security of the foreign  
intelligence activities of the United States and in order  
further to implement the proviso of section 102(d)(3) of  
this Act that the Director of Central Intelligence shall be  
responsible for protecting intelligence sources and methods  
from unauthorized disclosure--

(1) The Director of Central Intelligence shall  
promulgate rules and regulations for the protection  
of intelligence sources and methods from unauthorized  
disclosure.

*those classified means  
for obtaining*

(2) The term "intelligence sources" means  
[the purveyors of] <sup>FOREIGN intelligence</sup> information and materials [forming  
the basis of foreign intelligence.]

*these classified  
means for*

(3) The term "intelligence methods" means  
[the procedures, systems, devices or techniques  
used in gathering, assessing, analyzing, and]  
exploiting <sup>FOREIGN intelligence</sup> information and materials [forming the  
basis of foreign intelligence.]

[classified  
AUTHORIZED]

→ (1) The term "unauthorized person" means  
[ (4) Whoever <sup>knowingly</sup> possesses information relating  
to intelligence sources or methods is required [before  
[imparting] such information [to another person,] to  
-that the recipient is an authorized person-  
determine [and verify that such other person is law-  
fully entitled to receive it.]


(5) Whoever, being or having been an officer  
or employee of the United States Government, or being  
or having been a contractor of the United States Govern-  
ment, or being or having been an employee of a con-  
tractor of the United States Government, and in the  
course of such relationship becomes possessed of  
information relating to intelligence sources or methods  
which has been classified pursuant to Presidential  
Directive or rules and regulations promulgated by

the Director of Central Intelligence, knowingly <sup>COMMUNICATES</sup> directly or indirectly [imparts, discloses, publishes, divulges, or makes known in any manner,] or causes to be <sup>COMMUNICATED</sup> [imparted, disclosed, published, divulged, or made known in any manner,] such information or any part thereof to <sup>an unauthorized person</sup> [any person not entitled to receive it under law or executive order or rules and regulations of the Director of Central Intelligence] shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(6) Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts or practices which constitute, or will constitute, a violation of this <sup>SECTION</sup> ~~title~~, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with the provisions of this <sup>SECTION</sup> ~~title~~ or any regulation or order issued thereunder, and upon a showing by the Director of Central Intelligence that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary

injunction, restraining order, or other order may be  
granted.



 orig. drafts - 10 Nov. 72

25X1

SM

DRAFT:JDM:bg  
10 November 1972

NATIONAL SECURITY ACT AMENDMENTS OF 1973

CHAPTER \_\_\_\_\_ --PUBLIC LAW \_\_\_\_\_

[ ] H. R. [ ]

An Act to protect the security of the foreign intelligence  
activities of the United States

Be it enacted by the Senate and House of Representatives of the United  
States of America in Congress assembled,

Section 1. This Act may be cited as the National Security Act  
Amendments of 1973.

Section 2. Section 102 of the National Security Act of 1947,  
as amended, is amended by adding a new subsection (g) to read as  
follows:

(g) In the interests of the security of the foreign  
intelligence activities of the United States and in order  
further to implement the proviso of section 102(d)(3) of  
this Act that the Director of Central Intelligence shall be  
responsible for protecting intelligence sources and methods  
from unauthorized disclosure--

(1) The Director of Central Intelligence shall  
promulgate rules and regulations for the protection  
of intelligence sources and methods from unauthorized  
disclosure.

(2) The term "intelligence sources" means the purveyors of information and materials forming the basis of foreign intelligence.

(3) The term "intelligence methods" means the procedures, systems, devices or techniques used in gathering, assessing, analyzing, and exploiting information and materials forming the basis of foreign intelligence.

(4) Whoever possesses information relating to intelligence sources or methods is required, before imparting such information to another person, to determine and verify that such other person is lawfully entitled to receive it.

(5) Whoever, being or having been an officer or employee of the United States Government, or being or having been a contractor of the United States Government, or being or having been an employee of a contractor of the United States Government, and in the course of such relationship becomes possessed of information relating to intelligence sources or methods which has been classified pursuant to Presidential Directive or rules and regulations promulgated by

the Director of Central Intelligence, knowingly directly or indirectly imparts, discloses, publishes, divulges, or makes known in any manner, or causes to be imparted, disclosed, published, divulged, or made known in any manner, such information or any part thereof to any person not entitled to receive it under law or executive order or rules and regulations of the Director of Central Intelligence shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(6) Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts or practices which constitute, or will constitute, a violation of this <sup>SECTION</sup>~~title~~, or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing compliance with the provisions of this <sup>SECTION</sup>~~title~~ or any regulation or order issued thereunder, and upon a showing by the Director of Central Intelligence that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary

injunction, restraining order, or other order may be granted.

DRAFT:JDM:bg  
10 November 1972

NATIONAL SECURITY ACT AMENDMENTS OF 1973

CHAPTER \_\_\_\_\_ --PUBLIC LAW \_\_\_\_\_

   H. R.    /

An Act to protect the security of the foreign intelligence  
activities of the United States

Be it enacted by the Senate and House of Representatives of the United  
States of America in Congress assembled,

Section 1. This Act may be cited as the National Security  
Act Amendments of 1973.

Section 2. Section 102 of the National Security Act of 1947,  
as amended, is amended by adding a new subsection (g) to read as  
follows:

(g) In the interests of the security of the foreign  
intelligence activities of the United States and in order  
further to implement the proviso of section 102(d)(3) of  
this Act that the Director of Central Intelligence shall be  
responsible for protecting intelligence sources and methods  
from unauthorized disclosure--

(1) The Director of Central Intelligence shall  
promulgate rules and regulations for the protection  
of Intelligence Data from unauthorized disclosure.

(2) The term "Intelligence Data" means

(A) classified information and materials acquired, obtained, or used in intelligence activities of the United States concerning foreign countries and foreign nationals, and

(B) classified intelligence sources and methods

(3) The term "intelligence sources" means the purveyors of information and materials forming the basis of foreign intelligence.

(4) The term "intelligence methods" means the procedures, systems, devices or techniques used in gathering, assessing, analyzing, and exploiting information and materials forming the basis of foreign intelligence.

(5) Whoever possesses information relating to Intelligence Data is required, before imparting such information to another person, to determine and verify that such other person is lawfully entitled to receive such Intelligence Data.

(6) Whoever, being or having been an officer or employee of the United States Government, or being

or having been a contractor of the United States Government, or being or having been an employee of a contractor of the United States Government and in the course of such relationship becomes possessed of Intelligence Data, knowingly directly or indirectly imparts, discloses, publishes, divulges, or makes known in any manner, or causes to be imparted, disclosed, published, divulged, or made known in any manner, such Intelligence Data or any part thereof to any person not entitled to receive Intelligence Data under law or executive order or rules and regulations of the Director of Central Intelligence shall be fined not more than \$10,000 or imprisoned not more than ten years, or both.

(7) Whenever in the judgment of the Director of Central Intelligence any person has engaged or is about to engage in any acts or practices which constitute, or will constitute, a violation of this <sup>SECTION,</sup> ~~title,~~ or any regulation or order issued thereunder, the Attorney General on behalf of the United States may make application to the appropriate court for an order enjoining such acts or practices, or for an order enforcing



compliance with the provisions of this <sup>SECTION</sup> ~~title~~ or any regulation or order issued thereunder, and upon a showing by the Director of Central Intelligence that such person has engaged or is about to engage in any such acts or practices, a permanent or temporary injunction, restraining order, or other order may be granted.

§ 1112

FEDERAL CRIMINAL CODE

*Comment*

This section covers matters now dealt with in 18 U.S.C. § 2388. As under existing law, the proscription is limited to conduct occurring in time of war and accompanied by an intent adversely to affect United States military operations. The statement must be one of "fact"—that is, susceptible of proof of truth or falsity—as distinguished from political opinion. See *Pierce v. United States*, 252 U.S. 239 (1920). See Working Papers, pp. 446-47, 448-50.

§ 1112. Espionage.

(1) Offense. A person is guilty of espionage if he:

(a) reveals national security information to a foreign power or agent thereof with intent that such information be used in a manner prejudicial to the safety or interest of the United States; or

(b) in time of war, elicits, collects or records, or publishes or otherwise communicates national security information with intent that it be communicated to the enemy.

(2) Grading. Espionage is a Class A felony if committed in time of war or if the information directly concerns military missiles, space vessels, satellites, nuclear weaponry, early warning systems or other means of defense or retaliation against catastrophic enemy attack, war plans, or any other major element of defense strategy, including security intelligence. Otherwise espionage is a Class B felony.

(3) Attempt and Conspiracy. Attempted espionage and conspiracy to commit espionage are punishable equally with the completed offense. Without limiting the applicability of section 1001 (Criminal Attempt), any of the following acts is sufficient to constitute a substantial step under section 1001 toward commission of espionage under subsection (1)(a): obtaining, collecting, or eliciting national security information or entering a restricted area to obtain such information.

(4) Definitions. In this section:

(a) "national security information" means information regarding:

(i) the military capability of the United States or of a nation at war with a nation with which the United States is at war;

(ii) military or defense planning or operations of the United States;

(iii) military communications, research or development of the United States;

FINAL REPORT

§ 1113

(iv) restricted data as defined in 42 U.S.C. § 2014 (relating to atomic energy);

(v) security intelligence of the United States, including information relating to intelligence operations, activities, plans, estimates, analyses, sources and methods;

(vi) classified communications information as defined in section 1114;

(vii) in time of war, any other information relating to national defense which might be useful to the enemy;

(b) "military" connotes land, sea or air military and both offensive and defensive measures;

(c) "foreign power" includes any foreign government, faction, party, or military force, or persons purporting to act as such, whether or not recognized by the United States, any international organization, and any armed insurrection within the United States.

(d) "agent" means representative, officer, agent or employee or, in case of a nation, a subject or citizen.

*Comment*

This formulation of espionage substantially carries forward existing espionage statutes, 18 U.S.C. §§ 793-798. The term "reveals" is used in subsection (1)(a), however, to deal with problems raised in connection with the transmittal of information in the public domain. It permits a court to distinguish between the assembly and analysis of such information so as to constitute a revelation, and the simple transmittal of, for example, a daily newspaper. The culpability requirement of subsection (1)(a) is taken from 18 U.S.C. § 798. The definition of national security information in subsection (4)(a) is suggested by judicial construction of existing law. Note the inclusion of restricted data under the Atomic Energy Act and of intelligence and communications matters, now covered by 42 U.S.C. § 2274 and 18 U.S.C. §§ 798 and 952.

Subsection (2) changes the grading scheme of existing law in a manner similar to the change with respect to sabotage. See comment to § 1105, *supra*.

Subsection (3) grades attempts at the same level as the completed offense, which will not always be the case under the general attempt provision, § 1001. By specifying conduct sufficient to constitute an attempt (provided culpability is also present), this subsection eliminates the need for separate statutes dealing with those matters. Cf. 18 U.S.C. § 793 (a) and (b).

See Working Papers, pp. 450-54.

§ 1113. Mishandling National Security Information.

A person is guilty of a Class C felony if, in reckless disregard of potential injury to the national security of the United States, he:

§ 1114

FEDERAL CRIMINAL CODE

(a) knowingly reveals national security information to any one not authorized to receive it;

(b) violates a known duty, to which he is subject as a public servant, as to custody, care or disposition of national security information or as to reporting an unlawful removal, delivery, loss, destruction, or compromise of the security of such information; or

(c) knowingly having possession of a document or thing containing national security information, fails to deliver it on demand to a public servant of the United States entitled to receive it.

"National security information" has the meaning prescribed in section 1112(4).

*Comment*

This section deals with reckless mishandling of national security information in substantially the same manner as does existing law, under 18 U.S.C. § 793(c) (d) and (e) and other Title 18 provisions addressed to communication with reason to believe the conduct may injure the United States. This section also covers provisions on restricted data under the Atomic Energy Act and provisions dealing with intelligence and communications matters. See 42 U.S.C. § 2274; 18 U.S.C. §§ 798, 952.

See Working Papers, pp. 454-56.

§ 1114. Misuse of Classified Communications Information.

(1) Offense. A person is guilty of a Class C felony if he knowingly:

(a) communicates classified communications information or otherwise makes it available to an unauthorized person;

(b) publishes classified communications information; or

(c) uses classified communications information in a manner prejudicial to the safety or interest of the United States.

(2) Attempt and Conspiracy. Attempt and conspiracy to violate this section are punishable equally with the completed offense.

(3) Definitions. In this section:

(a) "communications information" means information:

(i) regarding the nature, preparation or use of any code, cipher or cryptographic system of the United States or of a foreign power;

(ii) regarding the design, construction, use, maintenance or repair of any device, apparatus or appliance used or

FINAL REPORT

§ 1114

prepared or planned for use by the United States or a foreign power for cryptographic or intelligence surveillance purposes;

(iii) regarding the intelligence surveillance activities of the United States or a foreign power; or

(iv) obtained by the process of intelligence surveillance from the communications of a foreign power;

(b) communications information is "classified" if, at the time the conduct is engaged in, the communications information is, for reasons of national security, specifically designated by a United States government agency for limited or restricted dissemination or distribution;

(c) "code," "cipher" and "cryptographic system" include, in addition to their usual meanings, any method of secret writing and any mechanical or electrical device or method used for the purpose of disguising or concealing the contents, significance or means of communications;

(d) "intelligence surveillance" means all procedures and methods used in the interception of communications and the obtaining of information from such communications by other than the intended recipients;

(e) "unauthorized person" means a person who, or agency which, is not authorized to receive communications information by the President or by the head of a United States government agency which is expressly designated by the President to engage in intelligence surveillance activities for the United States;

(f) "foreign power" has the meaning prescribed in section 1112(4).

(4) Congressional Use. This section shall not apply to the furnishing, upon lawful demand, of information to any regularly constituted committee of the Senate or House of Representatives of the United States or joint committee thereof. Inapplicability under this subsection is a defense.

*Comment*

This section substantially carries forward the provisions of 18 U.S.C. § 793. Subsection (1)(c), in present law, reads: "... in a manner prejudicial to the safety or interest of the United States or for the advantage of any foreign power to the injury of the United States." The latter phrase has been dropped as surplusage. The present law also contains the culpability requirement of "willfully," as well as

§ 1115

FEDERAL CRIMINAL CODE

"knowingly;" but that requirement, which would probably be "intentionally" under the Code formulations, has also been dropped. At the same time, however, the offense is graded somewhat lower than in present law (10 years), and the matters covered by this section are explicitly included in the definition of "national security information" in espionage (§ 1112), where intent to injure the United States is required and grading is at the Class A and B felony levels.

§ 1115. Communication of Classified Information by Public Servant.

(1) **Offense.** A public servant or former public servant is guilty of a Class C felony if he communicates classified information to an agent or representative of a foreign government or to an officer or member of an organization defined in 50 U.S.C. § 782(5) (communist organizations). "Classified information" means information the dissemination of which has been restricted by classification by the President or by the head of a United States government agency with the approval of the President as affecting the security of the United States.

(2) **Defenses.**

(a) It is a defense to a prosecution under this section that the public servant or former public servant was specifically authorized by the President or by the head of the United States government agency which he served to make the communication prohibited by this section.

(b) It is an affirmative defense to a prosecution under this section that the former public servant obtained the information in a manner unrelated to his having been a public servant or, if not so obtained, it was not classified while he was a public servant.

*Comment*

This section brings the provisions of 50 U.S.C. § 783(b) into Title 18, but extends the scope of the prohibitions to former public servants, subject to an appropriate affirmative defense. The section continues existing law in requiring proof only of intentional communication of classified information by a public servant to a foreign nation or the proscribed organization. No defense of faulty classification is provided. An alternative provision, prohibiting communication of classified information by anyone, together with a defense of inappropriate classification, has been considered. No need for a change from current policy to a broader prohibition, long rejected by the Congress, appears to have been established. See Working Papers, pp. 442, 450-53, 454-56, 457-61.

FINAL REPORT

§ 1118

§ 1116. Prohibited Recipients Obtaining Information.

An agent or representative of a foreign government or an officer or member of an organization defined in 50 U.S.C. § 782(5) (communist organizations) is guilty of a Class C felony if he:

- (a) knowingly obtains classified information, as defined in section 1115; or
- (b) solicits another to commit a crime defined in sections 1112, 1113, 1114 or 1115.

*Comment*

This section is the counterpart of § 1115 for certain recipients of sensitive information and provides Class C felony treatment of such persons when they solicit violations of §§ 1112 to 1115. See Working Papers, pp. 442, 450-56, 457, 458-61.

§ 1117. Wartime Censorship of Communications.

A person is guilty of a Class C felony if, in time of declared war and in violation of a statute of the United States, or regulation, rule or order issued pursuant thereto, he:

- (a) knowingly communicates or attempts to communicate with the enemy or an ally of the enemy;
- (b) knowingly evades or attempts to evade submission to censorship of any communication passing or intended to pass between the United States and a foreign nation;
- (c) uses any code or device with intent to conceal from censorship the meaning of a communication described in paragraphs (a) and (b); or
- (d) uses any mode of communication knowing it is prohibited by such statute or regulation, rule or order issued pursuant thereto.

*Comment*

This section brings into the Code the wartime censorship provisions of the Trading With the Enemy Act (50 U.S.C. App. § 3(c) and (d)). The Trading With the Enemy Act refers to "declared war;" and that limitation is continued here. See Working Papers, pp. 450-56, 457, 458-61.

§ 1118. Harboring or Concealing National Security Offenders.

A person is guilty of a Class C felony if he knowingly harbors or conceals another who has committed or is about to commit treason (section 1101), sabotage (section 1005), espionage (section 1112), or murder of the President or Vice President (section 1601).